DEPARTMENT OF STATE

FISCSAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

SMART Core Messaging Classified and Unclassified

Updated April 2008

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
E-mail: pia@state.gov

A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION

1) Does this system collect, maintain or disseminate personally identifiable information (PII) about individual members of the public? Personally identifiable information from/about individual members of the public means personally identifiable information from/about any person not acting in his/her official capacity as a federal government employee/contractor.

YES _X__ NO___

If the above answer is YES, please complete the survey in its entirety. If NO, complete the certification page and submit the PIA to the following e-mail address: pia@state.gov.

2) Does a Privacy Act system of records already exist?

YES ___ NO_X__

If yes, please provide the following:
System Name ____________________ Number ____

A Privacy system of records description is not required for this data.

3) What is the purpose of the system/application?

SMART replaces the Department of State's patchwork collection of outmoded and non-integrated messaging systems with a fully modernized, secure, integrated and effective messaging system that supports the Department's mission as well as the national security community. SMART provides an immediate, active searchable database of all foreign affairs and policy information as it is created, eliminating islands of inaccessible information and preserving the full record of foreign affairs.

4) What legal authority authorizes the purchase or development of this system/application?

The legal authority for SMART is derived from that of the Secretary of State, as defined in the Foreign Affairs Manual, Volume 1, *Organization and Functions*. See below.

1 FAM 012 THE SECRETARY OF STATE'S AUTHORITY

(TL:ORG-62; 01-31-1995)

a. The Secretary of State's basic authority derives from the provisions of the U.S. Constitution that vest in the President the authority to conduct foreign affairs. The Secretary of State is the President's principal foreign policy advisor and is responsible for the formulation of foreign policy and the execution of approved policy (22 U.S.C. 2656).

b. The Secretary exercises authorities under numerous statutes and executive orders, including the State Department Basic Authorities Act of 1980, 70 Stat. 890, as amended, the Foreign Service Act of 1980, Pub. L. 96-465, as amended, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Pub. L. 99-399), as amended.

c. In addition, the authorities of the Secretary of State include authority to administer the Department and the Foreign Service under 22 U.S.C. 2651a, 3921, and 3926, and E.O. 10973 and E.O. 12137.

C. DATA IN THE SYSTEM

1) What categories of individuals are covered in the system?

SMART may contain information for the following categories of individuals but is not limited to employees, contractors, and foreign nationals.

2) What are the sources of the information in the system?

SMART may contain information derived from a myriad of other systems to include but not be limited to:

- Department of State consular applications;
- Department of State human resources applications;
- Foreign countries information systems (e.g., driver licenses, marriage/death/birth reporting systems);
- Other U.S. Government agencies' applications; and
- World news media sources.

a. Who/what is the source of the information?

The SMART system allows all Department of State users and other tenant U.S. government agencies user rights to the system. Any user will be able to submit a message that could possibly contain PII.

b. What type of information is collected from the source of the information?

No information is physically collected from a source by SMART.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

SMART does not physically collect information from other sources. It is incumbent upon the drafter of the message to verify data for accuracy.

b. How will data be checked for completeness?

SMART does not physically collect information from other sources. It is incumbent upon the drafter of the message to verify the data for completeness.

c. **Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

SMART does not physically collect information from other sources. It is incumbent upon the drafter of the message to verify the data is current.

D. INTENDED USE OF THE DATA

1) **Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?**

Yes.

2) **Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?**

No.

3) **Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?**

N/A

4) **Will the new data be placed in the individual's record?**

N/A

5) **How will the new data be verified for relevance and accuracy?**

N/A

6) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

SMART messages can be retrieved via means of a user defined interest profile, organizational profiles that actively search the database for information necessary for SMART users to carry out their mission and via user defined ad-hoc full text searches. SMART will not use PII identifiers to provide search capabilities**.**

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

SMART provides a means of distributing and ad hoc text-based searching of information. No compilation, analysis or interpretation of the information is performed by the system.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

SMART is physically implemented using a primary and secondary site. One facility is located in the Washington, DC metropolitan area and the other is located at a suitable distance so that localized events do not disrupt service. Systems, operations and maintenance policies are consistent for both sites.

2) **What are the retention periods of data in this system?**
The retention period of data in SMART will be no longer then 25 years.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**
Removal from the system adheres to National Archive and Records Administration (NARA) guidance and both Department and National Security guidance regarding the handling of federal records and classified information. The SMART 300 was jointly developed with NARA to ensure that it properly integrates with and supports the objectives of the Office of Management and Budget (OMB) sponsored cross-agency e-records management initiative. There is also a memorandum of understanding (MOU) between NARA and the Department of State regarding the E-Records Management E-Government Initiative, Issue Area 4: Transfer of Permanent Electronic Records to support the development and implementation of electronic records management in the context of each agency's E-Government roles and responsibilities, including their roles and responsibilities regarding the Electronic Records Management Initiative, which is one of the 24 E-Government initiatives supporting the President's Management Agenda.

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
No

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**
N/A

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**
SMART will audit certain aspects of user-interaction (i.e., message creation, access, modification (versioning), delivery and non-repudiation, and disposition) storing audit information in a database. Audit reports will be available to authorized Department of State Diplomatic Security and management personnel.

SMART will utilize a role based access control methodology to ensure only personnel with appropriate authority can monitor usage of the system.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

No

8) **Are there forms associated with the system? YES ___ NO _X__**
If yes, do the forms include Privacy Act statements that include required information (e.g. legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

F. ACCESS TO DATA

1) **Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?**

System operators, system administrators and end-users (which includes but is not limited to contractors, full time employees, foreign national employees and other tenant U.S. government agencies residing in established Department of State facilities) with authorized clearances and established "need-to-know" requirements. Department of State authorized users will be able to access (search) the SMART repository (subject to security controls). Other agency personnel residing outside of Department of State facilities can be recipients of SMART messages, but will not have direct access to the SMART repository.

2) **What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access for individuals is governed by a role based access control methodology that enforces security clearance and "need-to-know" information access policies. These procedures, controls and responsibilities regarding access are now and will be documented in the Department of State Foreign Affairs Handbook (FAH), the Foreign Affairs Manual (FAM) and in the SMART Business Guide.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Access for individuals is governed by a role based access control methodology that enforces security clearance and "need-to-know" information access policies.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)**

SMART utilizes the current controls as listed in the FAM/FAH and will implement additional controls in the SMART Business Guide.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

Yes. Contractors are involved in the design, implementation, operation, use and maintenance of the system. Training for contractors is on the same level as employee training with regard to accessing and conveying official information. Necessary and appropriate privacy act clauses are contained in the SMART support contracts.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

There are no systems, internal or external, to the Department of State with direct access to the SMART repository.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**

There are systems external to the Department of State which interface with SMART and provide a means to exchange messages. However, these interfaces only allow for the direct addressing of messages to known users.

Release to other agencies is a routine occurrence, but occurs beyond the scope of this system. Information owners establish policy and process for all such distribution.

To control risk and liability associated with the distribution of sensitive or incorrect information, information owners strictly enforce the same clearance and "need-to-know" restrictions imposed by the system within the Department of State. There is no requirement for explicit State Department policy restrictions regarding general reuse of the information by other agencies. The U.S. government employs a consistent security clearance and "need-to-know" policy throughout the Executive Branch.

8) **Who is responsible for assuring proper use of the SHARED data?**

The message senders and receivers (i.e. users) of SMART are responsible for assuring proper use of the data, pursuant to applicable U.S. government and Department of State policies.

Messages with privacy-protected information (e.g. social security numbers) will be marked as sensitive, thereby protecting them from unauthorized distribution or searching.

Messages containing assessment of foreign governments, politics, or personalities may be posted, at the discretion of the originator, to SIPRNET. The posting provides access to the broader foreign affairs community, consonant with the information sharing policy of the Department of State and a soon-to-be-issued Executive Order.